

## STATEWIDE INFORMATION SYSTEMS POLICY

### Statewide Policy: Internet Filtering

**Product ID:** ENT-SEC-121

**Effective Date:** October 2004

**Approved:** Steve Bender, Acting Director, Department of Administration

**Replaces & Supersedes:** This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

### I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. [§2-17-505\(1\), MCA](#). It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. [§2-17-505\(2\), MCA](#).

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. [§2-17-512, MCA](#).

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. [§2-15-114, MCA](#).

## **II. Policy - Requirements**

### **A. Scope**

This policy applies to all computers that reside on the inside of the State's Internet firewall, including all state agencies as well as local government entities. This policy does not apply to colleges and universities, the Commissioner of Higher Education Office, or public access computers in libraries.

### **B. Purpose**

The Department of Administration Information Technology Services Division (ITSD) has the responsibility to insure that the state's telecommunications systems are used in the most effective and secure manner. To do so, ITSD believes that employees must understand the appropriate use of Internet resources. ITSD also finds that allowing access to certain types of web services or sites does not lead to effective and secure use of the systems. Therefore, ITSD adopts the following policy.

The purpose of this policy is to describe the steps to be taken to respond to requests for Internet filtering. This policy is to be used for all requests for Internet filtering, regardless of the agency or individual that is making the request.

### **C. Definitions**

*Agency* - Any State or local agency, or other entity that uses the State's Internet services.

*Internet Filtering* - The blocking, or prevention of access to a web site by users of the State's Internet services.

### **D. Requirements**

Internet filtering (or blocking) of individual web sites or general classes of sites will be instituted for the following reasons:

**ITSD Management Request.** ITSD management can request a web site or class of sites be blocked based on an analysis of web site access for the following reasons: 1) network performance, 2) an apparent violation of existing state or federal law or policy, or 3) security risks. Sites filtered will be those sites determined to not be needed by the majority of State employees to perform their job duties.

**Agency Request.** An agency can request a site or class of sites be blocked for a single device, group of devices or all of the devices in an agency. Agencies must make requests for blocking in writing to the Director of the Department of Administration.

A current list of web sites filtered is contained in Appendix A - Web Site Filters (at the end of this document). The sites or classes of sites filtered, is subject to

change at any time. ITSD will notify users of the state's Internet services prior to the implementation of a filter, unless it is deemed to be an emergency.

Agencies that have particular devices that need access to blocked sites can request that access be provided specifically to them. Agency requests must be received from the agency head. The request should be directed to the [ITSD Service Desk](#).

#### **E. Background - History On The Creation Of Or Changes To This Policy**

This policy was created by the Policy & Planning Services Bureau of the Information Technology Services Division.

This policy was distributed to the Information Technology Manager's Council, Information Technology Advisory Council and the SummitNet Executive Council for comment prior to adoption. This policy was updated by ITSD in 2004 because of the dissolution of the Council.

#### **F. Guidelines - Recommendations, Not Requirements**

All entities that use the state's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

#### **G. Change Control and Exceptions**

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an [Action Request](#) form. Requests for exceptions are made by submitting an [Exception Request](#) form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

### **III. Close**

For questions or comments about this instrument, contact the Information Technology Services Division at [ITSD Service Desk](#), or:

Chief Information Officer  
PO Box 200113  
Helena, MT 59620-0113  
(406) 444-2700  
FAX: (406) 444-2701

#### **IV. Cross-Reference Guide**

##### **A. State/Federal Laws**

- [2-17-505\(1\)](#) – Policy
- [2-17-514\(1\)](#) – Enforcement
- [§2-17-505\(2\), MCA](#)
- [§2-17-512, MCA](#)
- [§2-15-114, MCA](#)
- 2-17-302, MCA

##### **B. State Policies (IT Policies, MOM Policies, ARM Policies)**

- [2-15-112, MCA](#)
- ARM 2.13.102
- MOM 3-0620
- Internet Acceptable Use Policy
- SummitNet Acceptable Use Policy
- Transmission Privacy Policy
- User Responsibilities Policy
- [ARM 2.13.101 - 2.13.107](#) - Regulation of Communication Facilities
- [MOM 3-0130 Discipline](#)
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

##### **C. IT Procedures or Guidelines Supporting this Policy**

- [Policy: Establishing and Implementing Statewide Information Technology Policies and Standards](#)
- [Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards](#)

## V. Administrative Use

Product ID:	ENT-SEC-121
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	October 2004
Change & Review Contact:	<a href="#">ITSD Service Desk</a>
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: <ul style="list-style-type: none"><li>- Standardize instrument format and common components.</li><li>- Changed to reflect next review date.</li></ul>

# APPENDIX A

## VI. INTERNET FILTERING POLICY - WEB SITE FILTERS

Last Update: 01/10/03

This appendix identifies the individual and classes of web sites filtered by the State of Montana. The sites or classes of sites filtered is subject to change at any time with the approval of the State Chief Information Officer.

### A. Individual Sites

[www.webshots.com](http://www.webshots.com)

[www.kazaa.com](http://www.kazaa.com)

### B. Site Classes

Radio Stations - real audio

Sexually Explicit Material (pornography)

Hate Speech

Web proxy or anonymous sites

Non-standard email sites

Music distribution sites

Instant Messenger & Chat sites

Gambling sites

Adware/Spyware

Games

[Appendix A - Request for Agency Communications Records](#)